UNIT-I

Introduction to Blockchain technology

Blockchain could be a data structure that could be a growing list of information blocks. The knowledge blocks area unit coupled along, such recent blocks can’t be removed or altered. **Blockchain is the backbone Technology of Digital CryptoCurrency BitCoin. The blockchain is a distributed database of records of all transactions or digital event that have been executed and shared among participating parties. Each transaction verified by the majority of participants of the system. It contains every single record of each transaction.** BitCoin is the most popular cryptocurrency an example of the blockchain. Blockchain Technology first came to light when a person or Group of individuals name ‘Satoshi Nakamoto’ published a white paper on “*BitCoin: A peer-to-peer electronic cash system*” in 2008. Blockchain Technology Records Transaction in Digital Ledger which is distributed over the Network thus making it incorruptible. Anything of value like Land Assets, Cars, etc. can be recorded on Blockchain as a Transaction.

What is Blockchain?

A blockchain is a constantly growing ledger which keeps a permanent record of all the transactions that have taken place in a secure, chronological, and immutable way.

Let's breakdown the definition,

Ledger: It is a file that is constantly growing.

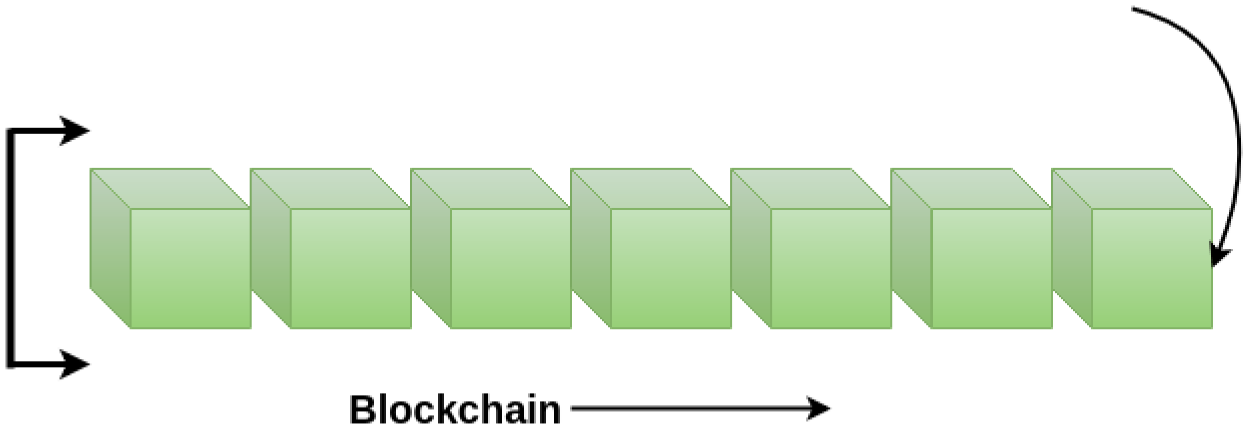
Permanent: It means once the transaction goes inside a blockchain, you can put up it permanently in the ledger.

Secure: Blockchain placed information in a secure way. It uses very advanced cryptography to make sure that the information is locked inside the blockchain.

Chronological: Chronological means every transaction happens after the previous one.

Immutable: It means as you build all the transaction onto the blockchain, this ledger can never be changed.

A blockchain is a chain of blocks which contain information. Each block records all of the recent transactions, and once completed goes into the blockchain as a permanent database. Each time a block gets completed, a new block is generated.



Note: A blockchain can be used for the secure transfer of money, property, contracts, etc. without requiring a third-party intermediary like bank or government. Blockchain is a software protocol, but it could not be run without the Internet (like SMTP used in email).

What Is a Block?

Every chain consists of multiple blocks and each block has three basic elements:

- The **data** in the block.
- The **nonce** — "number used only once." A nonce in blockchain is a whole number that's randomly generated when a block is created, which then generates a block header hash.
- The **hash** — a hash in blockchain is a number permanently attached to the nonce. For Bitcoin hashes, these values must start with a huge number of zeroes (i.e., be extremely small).

When the first block of a chain is created, a nonce generates the cryptographic hash. The data in the block is considered signed and forever tied to the nonce and hash unless it is mined.

What Is a Miner in Blockchain?

Miners create new blocks on the chain through a process called mining.

In a blockchain every block has its own unique nonce and hash, but also references the hash of the previous block in the chain, so mining a block isn't easy, especially on large chains.

Miners use special software to solve the incredibly complex math problem of finding a nonce that generates an accepted hash. Because the nonce is only 32 bits and the hash is 256, there are roughly four billion possible nonce-hash combinations that must be mined before the right one is found. When that happens miners are said to have found the "golden nonce" and their block is added to the chain.

Making a change to any block earlier in the chain requires re-mining not just the block with the change, but all of the blocks that come after. This is why it's extremely difficult to manipulate blockchain technology. Think of it as "safety in math" since finding golden nonces requires an enormous amount of time and computing power.

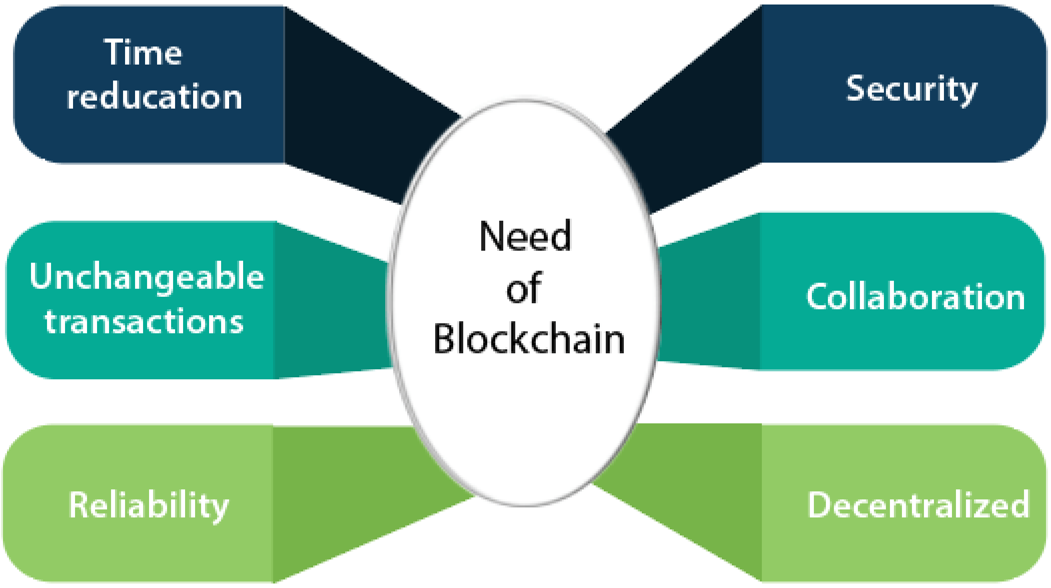
When a block is successfully mined, the change is accepted by all of the nodes on the network and the miner is rewarded financially.

> ***The whole point of using a blockchain is to let people — in particular, people who don't trust one another — share valuable data in a secure, tamperproof way***

Who uses the blockchain?

Blockchain technology can be integrated into multiple areas. The primary use of blockchains is as a distributed ledger for cryptocurrencies. It shows great promise across a wide range of business applications like Banking, Finance, Government, Healthcare, Insurance, Media and Entertainment, Retail, etc.

Need of Blockchain



Blockchain technology has become popular because of the following.

Time reduction: In the financial industry, blockchain can allow the quicker settlement of trades. It does not take a lengthy process for verification, settlement, and clearance. It is because of a single version of agreed-upon data available between all stakeholders.

Unchangeable transactions: Blockchain register transactions in a chronological order which certifies the unalterability of all operations, means when a new block is added to the chain of ledgers, it cannot be removed or modified.

Reliability: Blockchain certifies and verifies the identities of each interested parties. This removes double records, reducing rates and accelerates transactions.

Security: Blockchain uses very advanced cryptography to make sure that the information is locked inside the blockchain. It uses Distributed Ledger Technology where each party holds a copy of the original chain, so the system remains operative, even the large number of other nodes fall.

Collaboration: It allows each party to transact directly with each other without requiring a third-party intermediary.

Decentralized: It is decentralized because there is no central authority supervising anything. There are standards rules on how every node exchanges the blockchain information. This method ensures that all transactions are validated, and all valid transactions are added one by one.

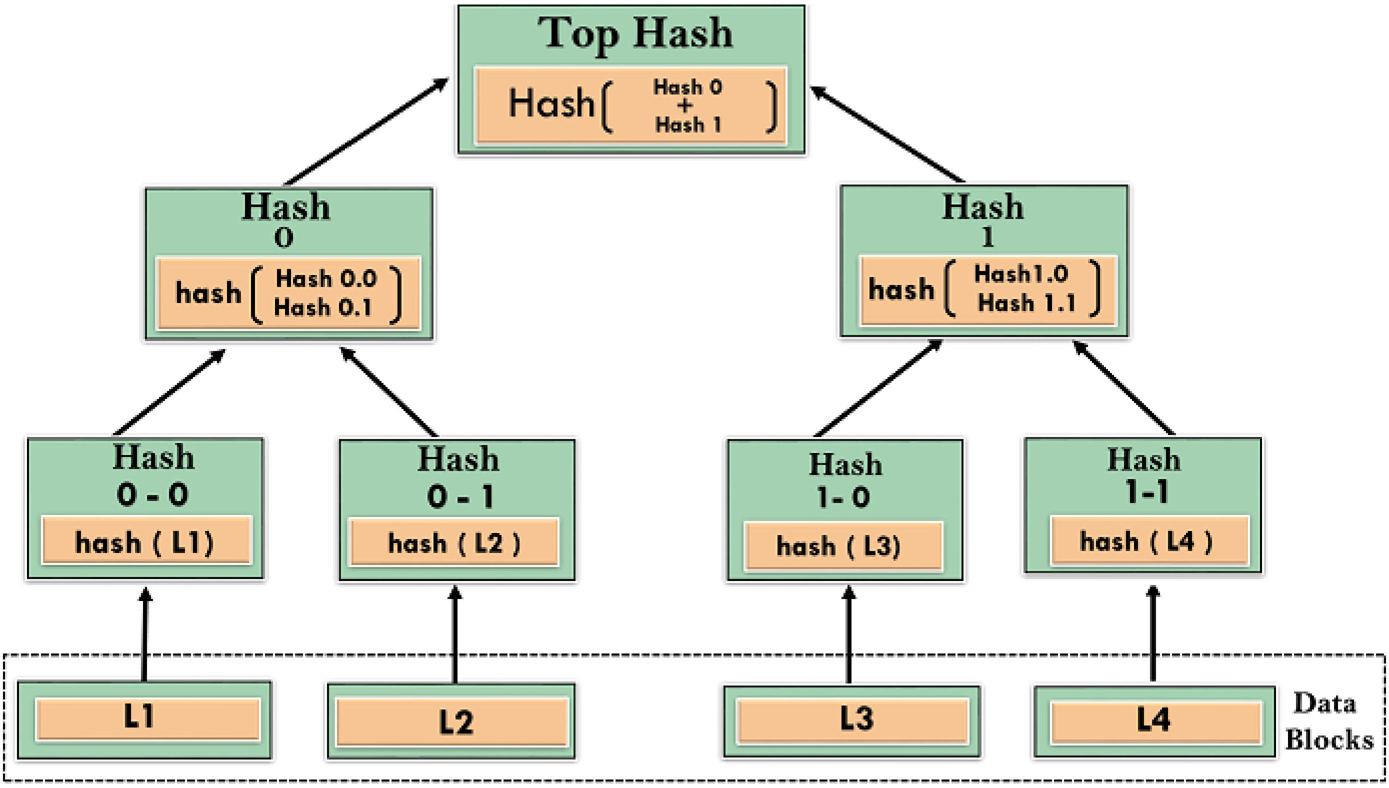
History of Blockchain

The blockchain technology was described in 1991 by the research scientist **Stuart Haber** and **W. Scott Stornetta**. They wanted to introduce a computationally practical solution for time-stamping digital documents so that they could not be backdated or tampered. They develop a system using the concept of **cryptographically** secured chain of blocks to store the time-stamped documents.

W. Scott Stornetta

Stuart Haber

In **1992**, Merkle Trees were incorporated into the design, which makes blockchain more efficient by allowing several documents to be collected into one block. **Merkle Trees** are used to create a 'secured chain of blocks.' It stored a series of data records, and each data records connected to the one before it. The newest record in this chain contains the history of the entire chain. However, this technology went unused, and the patent lapsed in 2004.



In **2004**, computer scientist and cryptographic activist **Hal Finney** introduced a system called **Reusable Proof Of Work (RPoW)** as a prototype for digital cash. It was a significant early step in the history of cryptocurrencies. The RPoW system worked by receiving a non-exchangeable or a non-fungible Hashcash based proof of work token in return, created an **RSA-signed** token that further could be transferred from person to person.

Hal Finney

RPoW solved the double-spending problem by keeping the ownership of tokens registered on a trusted server. This server was designed to allow users throug

Further, in 2008, **Satoshi Nakamoto** conceptualized the theory of **distributed blockchains**. He improves the design in a unique way to add blocks to the initial chain without requiring them to be signed by trusted parties. The modified trees would contain a secure history of data exchanges. It

Satoshi Nakamoto

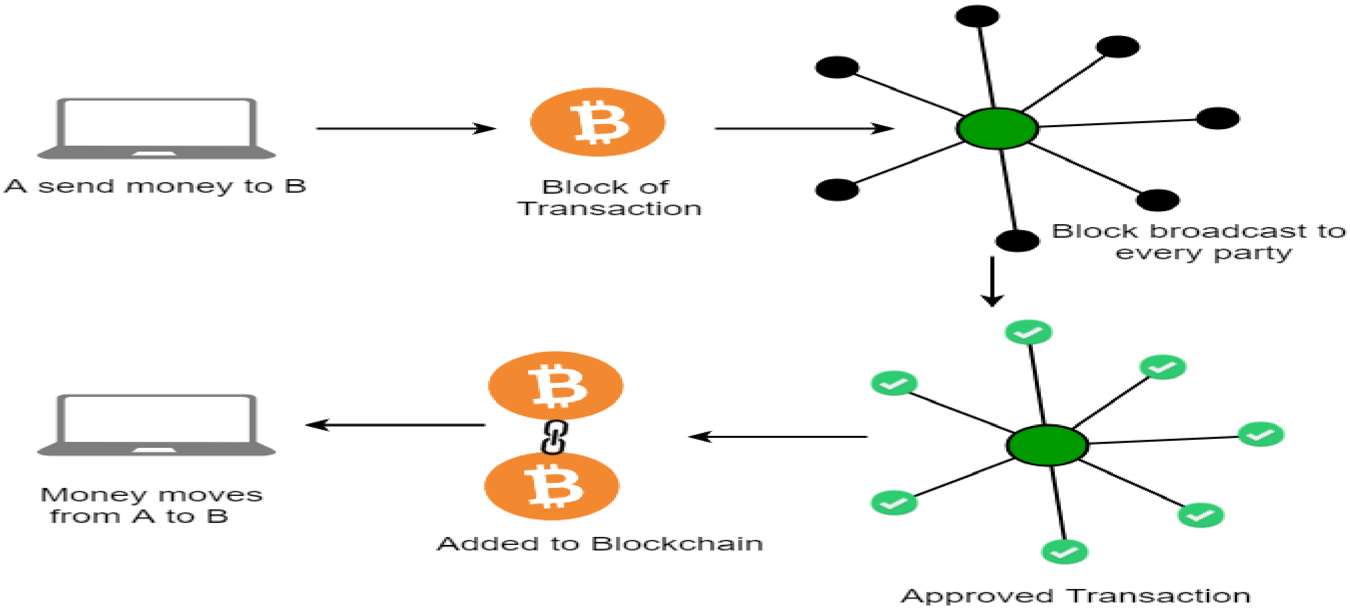
utilizes a peer-to-peer network for timestamping and verifying each exchange. It could be managed autonomously without requiring a central authority. These improvements were so beneficial that makes blockchains as the backbone of cryptocurrencies. Today, the design serves as the public ledger for all transactions in the cryptocurrency space.

The evolution of blockchains has been steady and promising. The words block and chain were used separately in Satoshi Nakamoto's original paper but were eventually popularized as a single word, the Blockchain, by **2016**. In recent time, the file size of cryptocurrency blockchain containing records of all transactions occurred on the network has grown from **20 GB** to **100 GB**.

How does Blockchain Technology work?

The goal of blockchain is to allow digital information to be recorded and distributed, but not edited. In this way, a blockchain is the foundation for immutable ledgers, or records of transactions that cannot be altered, deleted, or destroyed. This is why blockchains are also known as a distributed ledger technology (DLT).

One of the famous use of Blockchain is Bitcoin. Bitcoin is a cryptocurrency and is used to exchange digital assets online. Bitcoin uses cryptographic proof instead of third-party trust for two parties to execute transactions over the internet. Each transaction protects through digital signature.



As each transaction occurs, it is recorded as a “block” of data

Those transactions show the movement of an asset that can be tangible (a product) or intangible (intellectual). The data block can record the information of your choice: who, what, when, where, how much and even the condition — such as the temperature of a food shipment.

Each block is connected to the ones before and after it

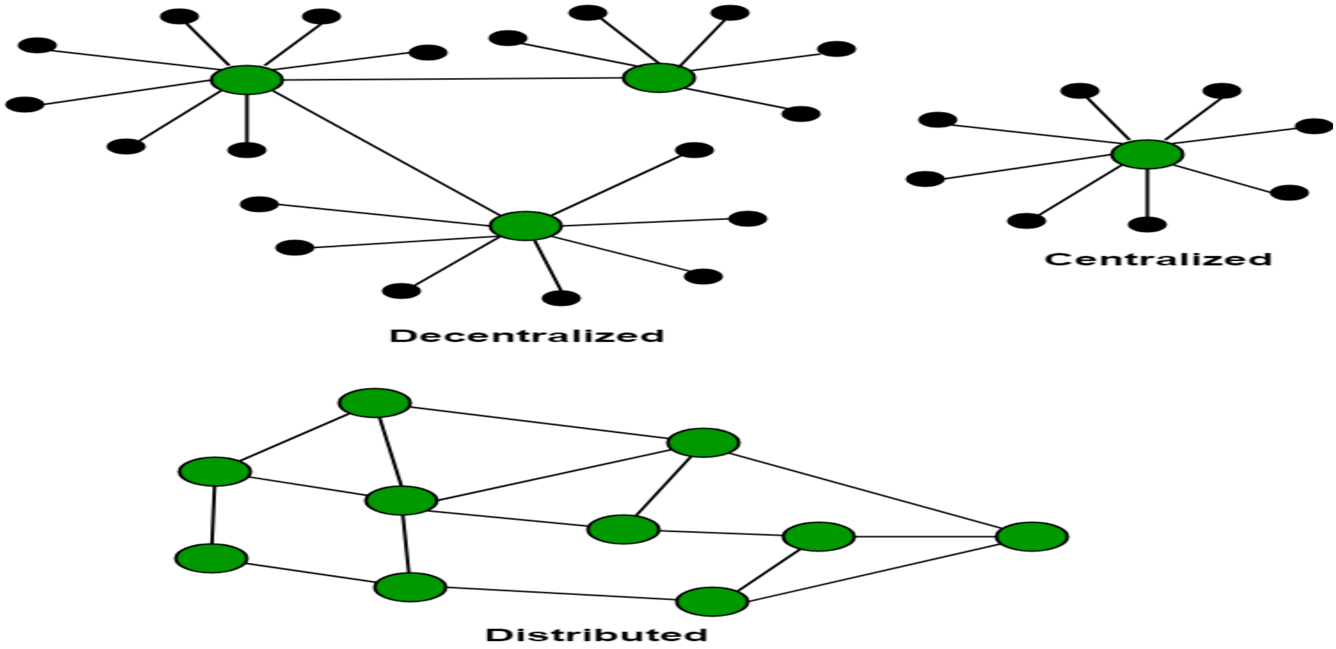
These blocks form a chain of data as an asset moves from place to place or ownership changes hands. The blocks confirm the exact time and sequence of transactions, and the blocks link securely together to prevent any block from being altered or a block being inserted between two existing blocks.

Transactions are blocked together in an irreversible chain: a blockchain

Each additional block strengthens the verification of the previous block and hence the entire blockchain. This renders the blockchain tamper-evident, delivering the key strength of immutability. This removes the possibility of tampering by a malicious actor — and builds a ledger of transactions you and other network members can trust.

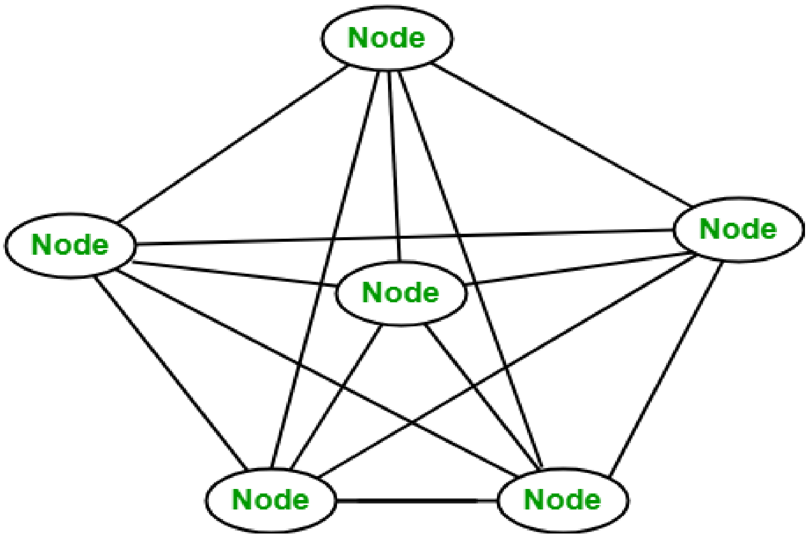
Distributed Database

There is no Central Server or System which keeps the data of the Blockchain. The data is distributed over Millions of Computers around the world which are connected to the Blockchain. This system allows Notarization of Data as it is present on every Node and is publicly verifiable.



A network of nodes:

A node is a computer connected to the Blockchain Network. Node gets connected with Blockchain using the client. Client helps in validating and propagating transaction on to the Blockchain. When a computer connects to the Blockchain, a copy of the Blockchain data gets downloaded into the system and the node comes in sync with the latest block of data on Blockchain. The Node connected to the Blockchain which helps in the execution of a Transaction in return for an incentive is called Miners.



Disadvantages of current transaction system:

- Cash can only be used in low amount transaction locally.
- Huge waiting time in the processing of transactions.
- Need to third party for verification and execution of Transaction make the process complex.
- If the Central Server like Banks is compromised, whole System is affected including the participants.
- Organization doing validation charge high process thus making the process expensive.

Building trust with Blockchain

Blockchain enhances trust across a business network. It's not that you can't trust those who you conduct business with its that you don't need to when operating on a Blockchain network. Blockchain builts trust through the following five attributes:

Distributed: The distributed ledger is shared and updated with every incoming transaction among the nodes connected to the Blockchain. All this is done in real-time as there is no central server controlling the data.

Secure: There is no unauthorized access to Blockchain made possible through Permissions and Cryptography.

Transparent: Because every node or participant in Blockchain has a copy of the Blockchain data, they have access to all transaction data. They themselves can verify the identities without the need for mediators.

Consensus-based: All relevant network participants must agree that a transaction is valid. This is achieved through the use of consensus algorithms.

Flexible: Smart Contracts which are executed based on certain conditions can be written into the platform. Blockchain Network can evolve in pace with business processes.

Benefits of Blockchain Technology

Time-saving: No central Authority verification needed for settlements making the process faster and cheaper.

Cost-saving: A Blockchain network reduces expenses in several ways. No need for third-party verification. Participants can share assets directly. Intermediaries are reduced. Transaction efforts are minimized as every participant has a copy of shared ledger.

Tighter security: No one can temper with Blockchain Data as it shared among millions of Participant. The system is safe against cybercrimes and Fraud.

Collaboration: It permits every party to interact directly with one another while not requiring third party negotiate.

Reliability: Blockchain certifies and verifies identities of every interested party. This removes double record, reducing rates and accelerate transactions.

Application of Blockchain

Leading Investment Banking Companies like Credit Suisse, JP Morgan Chase, Goldman Sachs and Citigroup have invested in Blockchain and are experimenting to improve the banking experience and secure it.

Following the Banking Sector, the Accountants are following the same path. Accountancy involves extensive data, including financial statements spreadsheets containing lots of personal and institutional data. Therefore, accounting can be layered with blockchain to easily track confidential and sensitive data and reduce human error and fraud. Industry Experts from Deloitte, PwC, KPMG and EY are proficiently working and using blockchain-based software.

Booking a Flight requires sensitive data ranging from the passenger's name, credit card numbers, immigration details, identification, destinations, and sometimes even accommodation and travel information. So the sensitive data can be secured using blockchain technology. Russian Airlines are working towards the same.

Various industries, including hotel services, pay a significant amount ranging from 18-22% of their revenue to third-party agencies. Using blockchain, the involvement of the middleman is cut short and allows interacting directly with the consumer ensuring benefits to both parties. Winding Tree works extensively with Lufthansa, AirFrance, AirCanada, and Etihad Airways to cut short third-party operators charging high fees.

Barclaysuses Blockchain to streamline the Know Your Customer (KYC) and Fund Transfer processes while filling patents against these features.

Visauses Blockchain to deal with business to business payment services.

Unileveruses Blockchain to track all their transactions in the supply chain and maintain the product's quality at every stage of the process.

Walmart has been using Blockchain Technology for quite some time to keep track of their food items coming right from farmers to the customer. They let the customer check the product's history right from its origin.

DHL and Accenture working together to track the origin of medicine until it reaches the consumer.

Pfizer,an industry leader, has developed a blockchain system to keep track of and manage the inventory of medicines.

The government of Dubai looking forward to making Dubai the first-ever city to rely on entirely and work using blockchain, even in their government office.

Along with the above organisations, leading tech companies like Google, Microsoft, Amazon, IBM, Facebook, TCS, Oracle, Samsung, NVIDIA, Accenture, PayPal, are working on Blockchain extensively.

Future scope of Blockchain Technology

Finance, supply chain management, and the internet of things are just a few of the sectors that blockchain technology has the power to upend (IoT). The following are some potential uses for blockchain in the future:

Digital Identity: Blockchain-based digital IDs might be used to store personal data safely and securely as well as offer a means of establishing identity without the need for a central authority.

Smart Contracts: A variety of legal and financial transactions could be automated using smart contracts, self-executing contracts with the terms of the agreement put straight into lines of code.

Decentralized Finance (DeFi): Using blockchain technology, decentralised financial systems might be built that support peer-to-peer transactions and do away with conventional intermediaries like banks.

Supply Chain Management: Blockchain technology can be applied to a permanent record of how goods and services have been moved, enabling improved openness and traceability across the whole supplychain.

Internet of Things (IoT): Blockchain technology may be used to build decentralised, secure networks for IoT devices, enabling them to exchange data and communicate with one another in an anonymous, safe manner.

In general, blockchain technology is still in its early stages and has a wide range of potential applications.

Types of blockchain networks

There are several ways to build a blockchain network. They can be public, private, permissioned or built by a consortium

Public blockchain networks

A public blockchain is one that anyone can join and participate in, such as Bitcoin. Drawbacks might include substantial computational power required, little or no privacy for transactions, and weak security. These are important considerations for enterprise use cases of blockchain.

Private blockchain networks

A private blockchain network, similar to a public blockchain network, is a decentralized peer-to-peer network. However, one organization governs the network, controlling who is allowed to participate, execute a consensus protocol and maintain the shared ledger. Depending on the use case, this can significantly boost trust and confidence between participants. A private blockchain can be run behind a corporate firewall and even be hosted on premises.

Permissioned blockchain networks (Hybrid)

Businesses who set up a private blockchain will generally set up a permissioned blockchain network. It is important to note that public blockchain networks can also be permissioned. This places restrictions on who is allowed to participate in the network and in what transactions. Participants need to obtain an invitation or permission to join.

Consortium blockchains

Multiple organizations can share the responsibilities of maintaining a blockchain. These pre-selected organizations determine who may submit transactions or access the data. A consortium blockchain is ideal for business when all participants need to be permissioned and have a shared responsibility for the blockchain.

Blockchain Challenges

Now it is time to understand the significant challenges of blockchain industry.

1. Scalability:

The ability to manage a large number of users at a single time is still a challenge for the blockchain industry. Blockchain technology involves several complex algorithms to process a single transaction. As of October 2017, the total number of coinbase users is recorded to be 11.7 million. As more and more people are getting used to it, the average transactions have also increased dramatically. It severely hit the processing speed of the transactions as a higher number of people implies more computers writing and accessing the network creating an overall cumbersome system.

2. Hackers and shadow dealing:

The one thing that the blockchain industry lacks is a set of regulatory oversight making it a volatile environment and an easy target for market manipulation. For instance, the infamous one coin scam where a lot of investors lost money thinking it to be the next revolutionary digital currency was revealed to be a Ponzi scheme scam. No matter how good you are with your cryptocurrency understanding, there is always a chance that the online wallet you are using may get hacked or be blocked by the government due to some shadowy practices.

3. Complex to understand and adopt:

Blockchain technology and the complexities it involves makes it hard for a layperson to understand and comprehend its benefits. Before diving into this revolutionary application, one needs to read it through and understand the principles of encryption and distributed ledger. Another point that makes blockchain hard to adopt is that financial institutions are adequate to provide secure payment gateways and other services at affordable prices compared to the costs incurred with blockchain.

4. Privacy:

Blockchain is an open ledger which is visible for everyone to view. It is an essential aspect in many cases, but it becomes a liability if used in a sensitive environment. Blockchain technology still has to go a long way to be adopted on a broad scale. The ledger needs to be remodeled in a way that allows restricted access and is accessible only to people who are authorized to view it.

5.Costs:

Blockchain is implemented usually for eliminating the expenses related to the third parties and intermediaries involved in the process of transferring values. Though, the blockchain technology is quite beneficial it is still in the nascent stages of innovation making it tough to integrate into the legacy systems. It makes it an expensive affair overall preventing its adoption by the government as well as private firms.

6. Blockchain is still a distant dream:

The market pundits are going gaga over the blockchain technology, its benefits and how it is re-shaping the infrastructure of emerging technologies like InsurTech and others. But, the truth is that the challenges mentioned above are still hard to conquer, and it will take some good time before blockchain becomes an integral part of all the industries.

The Blockchain is an innovative technology but needs a lot of technological advancements. However, technology has an intrinsic property of evolving and can always find a way through any challenges. So, we cannot say that blockchain is going anywhere anytime soon but will take time to revolutionize the technology sector completely.

What are peer-to-peer (P2P) networks?

Peer-to-Peer (P2P) technology is based on the decentralization concept, which lets network participants conduct transactions without needing any middle-man, intermediaries or central server. Peer-to-peer technology is how Bitcoin (BTC) operates; no administrator is required to maintain track of user transactions on the network. Instead, the peers in the network cooperate to handle deals and manage the BTC.

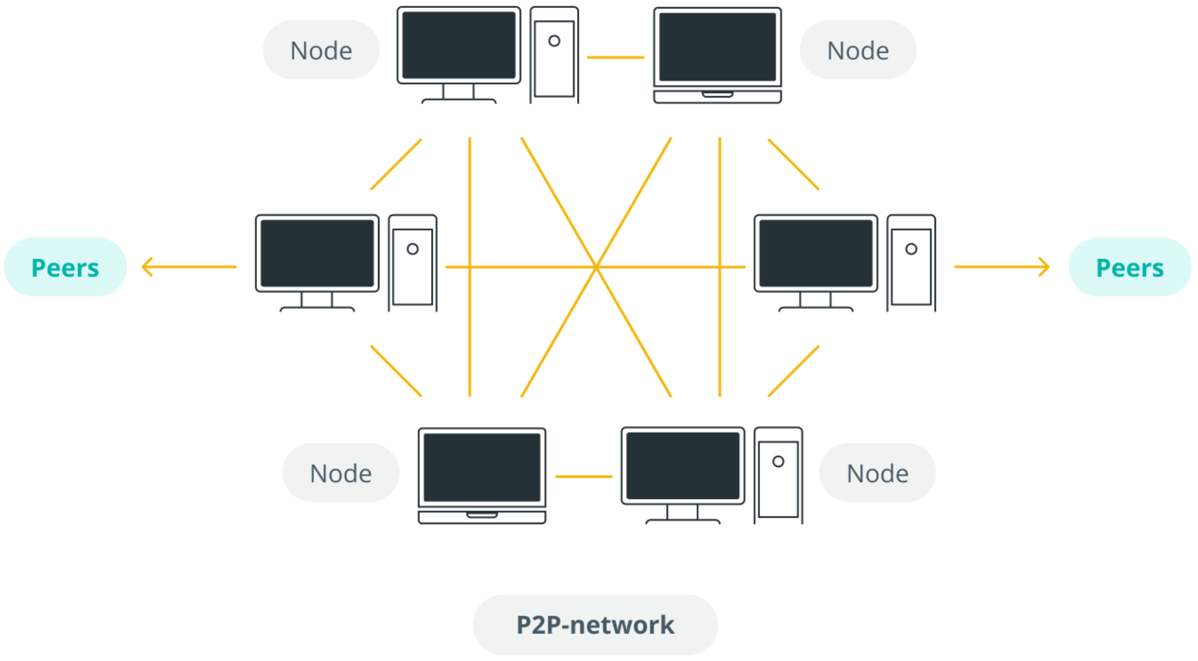
Peers refer to the nodes or computers that perform the same tasks and have the same power within a blockchain network. Blockchain is a P2P network that acts as a decentralized ledger for one or more digital assets, which refers to a decentralized peer-to-peer system where each computer keeps a complete copy of the ledger and verifies its authenticity with other nodes to guarantee the data is accurate. In contrast, transactions at a bank are kept secret and are only overseen by the bank.

The security of the underlying consensus algorithms and the privacy of transactions are all closely tied to its implementation, making the P2P network a crucial component of blockchains. However, no common P2P protocol for blockchains has been suggested. Instead, different cryptocurrencies have developed and adapted their own peer-to-peer protocols.

How do P2P networks work?

As mentioned, there are no central in peer-to-peer blockchain networks. Instead, all nodes (peers) are connected to one another. A mesh network with a “flat” topology connects the network nodes and there is no hierarchy. In a peer-to-peer network, nodes simultaneously give and consume services with reciprocity serving as the motivation for participation, making P2P networks open, decentralized and robust by nature.

Diagrammatic representation of a peer-to-peer network



cointelegraph.com

Each node on the network must serve as both a client and a server to other nodes in a P2P network, making it distinct from a traditional client-server setup. There is always a central server in a client-server configuration from which the client downloads files.

On the contrary, in a decentralized setup, each node acts as a server that can download files and share them with other nodes. A node may perform both the sharing and receiving functions concurrently, which accounts for the P2P network’s speed, security and efficiency.

What are the various types of peer-to-peer (P2P) networks?

A P2P architecture can be categorized into structured, unstructured and hybrid peer-to-peer networks, as explained below.

Structured peer-to-peer networks

In this type of network, nodes interact based on an organized structure, enabling nodes to precisely search for files, even if the content is unavailable. However, due to an organized system, some sort of centralization exists in structured P2P networks. Unlike unstructured peer-to-peer networks, structured peer-to-peer networks are challenging to set up, although they provide simple data access.

Unstructured peer-to-peer networks

There is no set structure for the nodes in this kind of network, allowing network participants to join or leave the network as they desire. Also, due to a lack of definite structure, participants converse with one another at random. However, unstructured P2P networks require all nodes to remain active to power a high number of transactions, mandating huge CPU power to ensure that the network runs properly.

Hybrid peer-to-peer networks

This type of P2P network mixes some P2P design aspects with the traditional client-server approach. For example, it makes it possible to locate a node using the central server. A distributed network application framework called the client-server architecture assigns tasks to servers and clients in the same system that connect via a computer network or the Internet.

Benefits of P2P blockchain networks

Peer-to-peer networks offer many benefits over the traditional client-server architecture as there is no single point of failure in a distributed network of computers. On the other hand, data may get erased if the server goes down in a client-server model. Moreover, P2P networks may withstand attacks reasonably well since they are decentralized and lack a centralized server. Unlike banks, blockchains using P2P architecture cannot restrict network participants from doing a transaction.

In addition, P2P networks are cost-effective because they do not require a network operating system, thus reducing costs. Furthermore, peer-to-peer networks are remarkably resilient to changes in peer composition — the network can readily accommodate an increase in load if many new peers join it at once. Also, the loss of a single peer has little effect on the network as a whole.

Various use cases of P2P blockchain networks include sharing software and games through file-sharing networks. Cryptocurrencies also use P2P networks to allow users to conduct transactions in a decentralized setup. Other than the Bitcoin network, Skype and BitTorrent are P2P network examples.

Limitations of P2P blockchain networks

Despite the above advantages, peer-to-peer networks are not without any cons. As there is no centralized server, any virus or malware may get injected into all the participating nodes from the infected one. Similarly, nodes can distribute copyrighted content as no centralized party controls the system.

Additionally, anyone can create parallel networks called a hard fork of the blockchain if they want, implying that the software needs to be updated to comply with the new guidelines. For instance, following the Ethereum Merge, proof-of-work Ethereum (ETHW) was created by a Chinese miner.

P2P networks frequently have a sizable number of users who consume the resources shared by other nodes while keeping their own resources to themselves. Such free-riding nodes are called “leechers” that may support unethical and immoral behavior.

Hashing And Digital Signature In Blockchain

Want to know how the highest level of security is implemented in blockchain? Hashing and Digital Signature are the important terms that bring desired security level in blockchain with cryptography. Let’s learn what is hashing and digital signature in blockchain.

Security is one of the prominent requirements in the present times, with businesses wondering about innovative approaches for safeguarding information. One of the most innovative solutions that have emerged recently for helping businesses in secure information exchange points towards blockchain. Blockchain technology brings functionalities of distributed ledger and ensures that unauthorized parties couldn’t see the information exchanged in a specific transaction.

It uses cryptography to provide the desired security while bringing attention towards hashing and digital signature in blockchain. Both hashing and digital signature have a huge role to play in the blockchain landscape. The following discussion aims to shed light on the importance of hashing and digital signature for blockchain.

The most important aspect in discussions around hashing and digital signature in blockchain primarily revolves around cryptography. Communication has evolved gradually over the years as we have come from pictograms to flash storage devices storing massive information. However, communications have always been following best practices of encryption to ensure that information is not visible to other individuals.

Therefore, cryptography emerged as a vital solution for ensuring safeguards for sensitive information. Cryptography involves scrambling the original content of the message to a cipher before sending it to the recipient. The recipient could use keys for unlocking the cipher, and the keys are available only with the recipient. Therefore, any other party couldn't intercept the communication in the course of its journey from sender to recipient.

What is Hashing and Digital Signature in the Blockchain?

Blockchain relies largely on cryptography as a major selling point. It is also interesting to note the definition of hashing in blockchain and the role of digital signatures in understanding how they fit in the blockchain equation. Let us start with hashing first.

What is Hashing in Blockchain?

Hashing is the process of taking an unlimited amount of input data and leveraging it for the creation of specific amounts of output data. The input data does not have any fixed size, thereby offering considerable flexibility in the selection of inputs for hashing. In addition, the importance of hashing in blockchain security is visible in the requirement of hashing for adding blocks. You should also note that there are various hashing algorithms tailored for varying requirements of users.

Interestingly, hashes have found a wide range of applications in various use cases, with the most prominent example referring to digital fingerprinting. Digital fingerprinting is just the same as an actual fingerprint, and the hashing in digital fingerprints serves as the best instrument for verifying the fingerprint.

The hash helps in offering confirmation regarding the production of output from the hashing procedure. In addition, the hash also confirms that the output of the procedure has not been subject to any unwanted tampering. The verification process generally involves calculations for confirming matches between hashes and the originally published content. Any form of mismatch could clearly showcase evidence of modification or tampering in the output hash.

Hashing refers to the transformation and generation of input data of any length into a string of a fixed size, which is performed by a specific algorithm. In particular, the Bitcoin hash algorithm is SHA-256 or Secure Hashing Algorithm 256 bits. This algorithm is a one-way cryptographic function as the original data cannot be retrieved via decryption.

The implementation of a cryptographic hash function is beneficial to prevent fraudulent transactions, double spending in blockchain, and store passwords. But, what is Bitcoin hash, and what does it have to do when put in this context? In short, this is a unique number that is not duplicable according to the algorithm. Therefore, it is frequently used to verify a file's authenticity. To put it in context, when there's a change in a hashed file, its hash will automatically change as well. And each subsequent hash is tied to the previous hash, thus ensuring the consistency of all blocks.

How Hashing Works in Blockchain

So what is a hashing algorithm in blockchain, and how does it work? In a nutshell, a hashing algorithm takes an infinite number of bits, performs calculations on them, and outputs a fixed number of bits. Regardless of the input data's length, the output will always be rectified. As a result, the original data is called input, and the final transformation is called a hash. Today, many hashing algorithms differ only in the way information is processed.

To fully comprehend what hashing is about, it's essential first to understand the data structure. A data structure is a specific way of storing data that consists of two key elements: pointers and linked lists. Pointers are variables referring to other variables, so they act as indicators that show the way to the right location. Besides, it provides the address of the next block in the chain. Linked lists, on the other hand, make up a sequence of the nodes that are connected with the help of pointers.

Thanks to hashing in the blockchain, each block is assigned an original identifier, which will entail the irreversible consequences of changing the blockchain. The block is identified by information included in the header of the block. It consists of such details as:

- the version number of the blockchain
- UNIX timestamp
- hash pointers
- nonce, which is the value the miners need to create a block
- a hash of a Merkle root

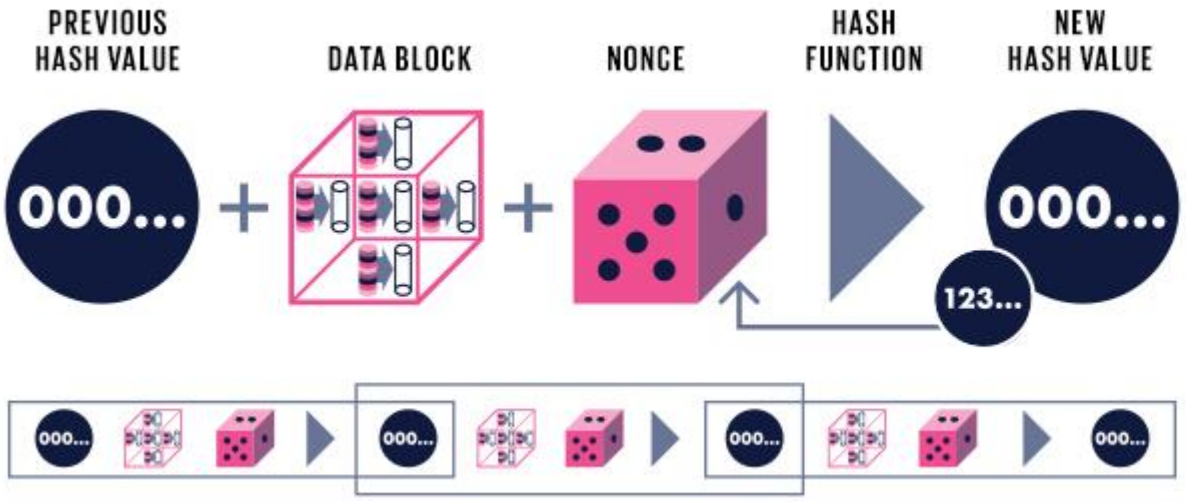
All these elements are needed to create the block. So when a hash happens to the blockchain, the data will be converted into a unique string within a block.

How to Solve a Hash?

To solve a hash, it begins with solving complex mathematical problems containing data in the block header. But before a miner initiates the process, they'll need to carry out a trial-and-error process to decide which string to use as a nonce. When a nonce is identified, miners will focus on the nonce (a string number) that is related to the previous block's hashed content. In order for a hash to be considered successful, the new hash needs to be less than or equal to the target hash. And in exchange, the miner will get a reward to add the block into the blockchain.

The Relationship of Proof of Work in Hashing

Proof of Work (PoW) algorithm is correlated to the blockchain hash as this algorithm is useful to confirm transactions and produce new blocks to the chain.



Applications of Hashing in Blockchain

The use of hashing in blockchain in such cases points out clarity on tamper-proofing. Every new blockchain begins with a genesis block which is responsible for capturing data regarding almost anything that has happened on the blockchain to date. As a result, the output of a hash function directly points out the most recent state of the concerning blockchain.

It is also important to note that activities are added subsequently to the chain as they happen. Most important of all, the new blocks always capture details associated with the previous block. Any form of modification could change the hash of the chain, thereby helping in easier and precise identification.

Hashing in cryptography and blockchain is primarily a one-way function that features a properly crafted algorithm without any concerns for reversal of hashing process and exposure of original input. Therefore, hashing can provide a substantial advantage over the two-way function in encryption that enables encryption and decryption through the suitable keys or key-pairs.

Another profound application of hash functions is clearly evident in data structures where you can find bloom filters or hash tables. In such cases, the objective of hashing focuses on faster data lookup rather than security. On the other hand, hash functions also find applications in the context of digital signatures where they are ideal for producing the same output for the same input with a deterministic approach.

As a result, the use of hashing and digital signature in blockchain could help recipients in recomputing the output of a hash function with the same hash function. The comparison of the message digest with the transmitted digest could help in verifying that the message didn't go through unwanted modifications in transit.

Even if the message features minor differences in punctuation, content, or spacing, the message digest in the output would have radical differences. In addition, it is difficult to find out the level of difference between two different messages through comparison of the digest. As you must have understood, the smallest difference in inputs could result in a completely unique digest value.

So, it is quite clear that hashing has a formidable significance for cryptography in the blockchain. However, the applications of hashing in blockchain have to follow certain important requirements such as,

1. Input could feature variable length
2. Output must have a fixed length
3. The hash function for any specific input presents relative ease of computing.
4. Hash function features the collision-free trait, which ensures that you could not have two different messages that produce a similar hash value.
5. Hash function is always one-way and clearly implies the extreme difficulty associated with determining the input by referring to the output.

Hashing Algorithms

With a clear idea regarding the significance of hashing in blockchain, it is important to know about hashing algorithms. The secure hashing algorithm or SHA is the most common hash function recommended by the National Institute of Standards and Technology (NIST). The notable successors of SHA such as SHA-1, SHA-2, and SHA-3 have gained profound recognition for their capabilities. Let us take a look at their details.

SHA-1 could take input of practically any length and then generate a 160-bit message alongside processing messages in blocks of 512-bit size. If message length is not a multiple of 512-bit, then the SHA algorithm could pad up the message with data so that it could reach the next closest multiple of 512-bit.

SHA-2 is presently one of the favorite algorithms in the cryptography community, although with certain setbacks like in the SHA-1 algorithm. After its introduction in 2001, SHA-2 has been through substantial changes over the years with the arrival of four variants. The four different variants include SHA-256, SHA-224, SHA-512, and SHA-384, with SHA-256 being a widely adopted cryptographic algorithm.

SHA-256 can create a 256-bit message digest through the use of 512-bit block size, while SHA-224 utilizes a truncated version of SHA-256 for creating a 224-bit message digest using the 512-bit block size. SHA-512 could create a 512-bit message digest by using the 1024-bit block size, and SHA-384 utilizes a truncated version of SHA-512. SHA-384 can generate a 384-bit message digest by leveraging a 1024-bit block size.

The SHA-3 algorithms are the latest additions in secure hashing algorithms showing the importance of hashing in blockchain. SHA-3 came into existence in 2015 and fall on the same lines as MD5 algorithm standards. It has the capability to serve as a replacement for SHA-2 while also offering similar variants and hash lengths. The only difference of SHA-3 is that it presents possibilities of better security.

▪

MD2- Message Digest

The MD2 Message Digest algorithm came forward in 1989 as an alternative for offering secure hash functions for 8-bit processors. MD2 helps in padding up the message to the length of multiples of 16-bit and the creation of a 16-byte checksum.

MD4 is an enhanced alternative to MD2 and provides padding for a message to a length that is 64-bit smaller than 512-bit multiples. Subsequently, it could process 512-bit blocks of the message in different rounds for producing a 128-bit message digest.

MD5 is the latest version of message digest algorithm and could offer the same padding requirements as MD4. In addition, it brings some additional security features which end up reducing the speed of producing message digest.

Digital Signature in Blockchain

Digital signatures are basically cryptographic proof systems that can help in establishing trust on the blockchain. Trust in the blockchain system could ensure proving that the message could originate from a particular source, thereby ruling out any concerns of hacking or other discrepancies. Digital signatures can be considered as the digital counterparts of stamped seals or handwritten signatures.

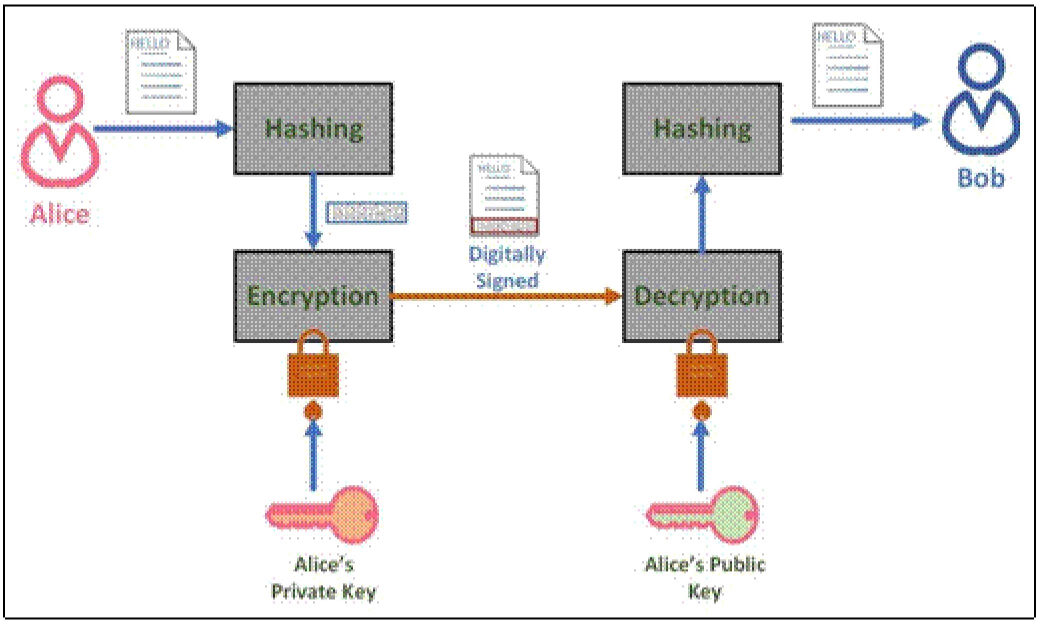
However, they are capable of offering better security with the reduced possibility of identity theft or impersonation. Digital signatures follow the specific precedents of asymmetric cryptography by linking two different keys with mathematical links. The keys include a private key and a public key. It is possible to deploy a digital signature system with the help of a secure hash function. The importance of a digital signature in blockchain largely revolves around two primary objectives such as,

1. Digital signatures ensure that the message received by a recipient has come from the sender claiming to have sent the information. The property is known as non-repudiation.
2. Digital signatures also provide assurance to recipients about the fact that messages have not been through any modifications in transit. As a result, infrastructures can find better safeguards against malicious intermediaries or unintentional modifications.

Digital signature

A **digital signature** is a set of algorithms for determining the authenticity and integrity of digital messages or documents. It assures the recipient that the message was indeed created by the expected sender and that the message was not altered during transmission. The sender cannot deny having sent the message.

When **Alice** sends a document to **Bob**, she will follow certain steps to digitally sign the document, as shown in the following diagram:



These steps are as follows:

1. Calculate the message digest of the document Alice wants to send to Bob with a cryptographic hash function, usually MD5 or any SHA algorithm.
2. Encrypt the message digest with Alice's private key, append the encrypted message digest to the original document, and send the combined message out.
3. Once Bob receives the combined message from Alice, he will separate the encrypted message digest from the document itself. Bob will use Alice's public key to decrypt the encrypted message digest.
4. At the same time, Bob will calculate the message digest of the received document and compare the resulting message digest with the decrypted message digest to see whether there is a match. If yes, Bob is assured that the document originated from Alice without any tampering.

In blockchain, a digital signature is a way to prove ownership of the underlying cryptocurrency or electronic coin. When Alice needs to pay Bob 10 BTC, she will digitally sign a hash of the previous transaction, which can prove that Alice has ownership of the 10 BTC.

In summary, cryptography is one of three foundational pillars in blockchain technology. Public key cryptography is the basis for blockchain wallets and transactions, and the cryptographic hash function is a key element underpinning the PoW consensus mechanism. A digital signature is used as proof of ownership of the underline electronic coins or cryptocurrency.

Relationship between Hashing and Digital Signatures

Now that you know ‘what is hashing and digital signature in the blockchain?’ it is important to find out the link between them. In the case of blockchain, a digital signature system focuses on three basic phases such as hashing, signature, and verification. Let us take a look at the working of a blockchain-based digital signature.

Step 1: First of all, the blockchain hashes the message or digital data through the submission of data via a hashing algorithm. The algorithm helps in generating a hash value or the message digest with messages differing profoundly in size only to give the same length of hash values upon hashing. As we already know, this is the most fundamental trait in a hash function and exhibits a clear influence on digital signatures. Hashing is mandatory in most blockchain applications for the flexibility in using fixed-length message digests for the complete process.

Step 2: The next step in the working of digital signature in blockchain refers to signing. The sender of the message must sign it after hashing of information in the message. At this point of the process, public key cryptography plays a critical role. Many digital signature algorithms offer unique mechanisms, albeit with the single approach of asymmetric cryptography. Since digital signatures are related directly to the content in each message, digitally signed messages are likely to have different digital signatures.

Step 3: The final step in the use of blockchain-based digital signature refers to verification. Recipients could easily check the validity of digital signatures through the use of a public key. The signature could work as a unique digital fingerprint of the concerned message. However, it is also important to pay attention to the secure storage and management of keys for avoiding unwanted circumstances.

The applications of digital signature in blockchain could help in achieving the important results of non-repudiation, authentication, and data integrity. As a result, hashing and digital signatures have prominent contributions in improving the security of blockchain applications.

What is Public Key Cryptography?

Public key cryptography is a security protocol that ensures the safety of data that we exchange through a transaction in a blockchain network. The aspect of security is crucial in a point-to-point network like blockchain. Because, in such a network, nodes do not personally know and trust each other. There is a need for a robust security system in place. One which secures the information they are sending or receiving without worrying about security breaches. Also, this eliminates the need for all the nodes to know and trust each other personally.

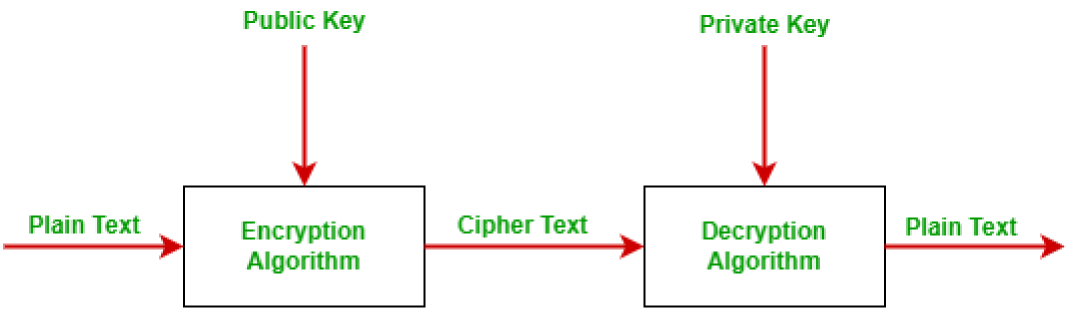
Public key cryptography is an asymmetric type of cryptography where we use a pair of keys (*public key* and *private key*). It uses them to encrypt/decrypt the information and verify the users. The process of public-key cryptography ensures two things i.e,

1. Encryption of the information at the sender's end using the public key (of the receiver). This ensures that no third party can access or understand the encrypted information in or out of the network. Only the intended receiver can decrypt and read the message using its own private key.

2. Signing the message or information for verification using the sender's private key. This authenticates the identity of the sender and states that he is a legitimate node in the blockchain network. The receiver verifies this by using the public key of the sender. This verification process of users in a network is done through digital signatures.

Thus, public-key cryptography is a way of providing a digital identity to the user. Through this one can carry out secure transactions within a blockchain network. Now let us understand exactly how this happens.

Most of the time blockchain uses public-key cryptography, also known as asymmetric-key cryptography. Public key cryptography uses both public key and private key in order to encrypt and decrypt data. The public key can be distributed commonly but the private key can not be shared with anyone. It is commonly used for two users or two servers in a secure way.



Public Key: Public keys are designed to be public. They can be freely given to everyone or posted on the internet. By using the public key, one can encrypt the plain text message into the cipher text. It is also used to verify the sender authentication. In simple words, one can say that a public key is used for closing the lock.

Private Key: The private key is totally opposite of the public key. The private key is always kept secret and never shared. Using this key we decrypt cipher text messages into plain text. In simple words, one can say that the public is used for opening the lock.

There are three key elements in public-key cryptography i.e. (i) *Pair of keys; Private and public key*, (ii) *Cryptography wallet* and *wallet address*, and (iii) *Digital signature*. Each of these three elements contributes significantly to creating an authentic digital identity just like our bank account, account number, and password. The only difference here is that it is to exchange information or cryptocurrency within a blockchain network.

Public key cryptography uses special algorithms to create these keys. These algorithms work in a unidirectional manner, i.e. the algorithm will first create a private key from it, a public key, and from it, a public address. We cannot reverse the order of generation i.e. we cannot compute the private key from a public key or wallet address from the public key.

This ensures the security of the public key cryptography system even more. It is because the public key and public address are made public to carry out transaction and verification processes.

Therefore, public-key cryptography ensures the integrity of the information, the authenticity of the user, and the legitimacy of the transaction. A private key is like an account password for a user. One can decrypt a coded message sent to them and make a digital signature from it for verification.

A public key is open for the network which others use to verify a transaction and encrypt a message. Thus, whenever a transaction takes place between two nodes, the private and public keys of both the nodes take part in making the transaction secure. It does so by encrypting the information and verifying the user by their digital signature. This double layer of protection makes public-key cryptography the best security system for blockchain.

Why Do We Need Public-Key Cryptography?

- In symmetric-key cryptography, a single key is used to encrypt and decrypt the message. Here, the possibility of data loss or unauthorized access to data is high. To overcome the unauthorized access of data and data sent securely without any loss, we use public-key cryptography.
- Public-key cryptography is more secure than symmetric key cryptography because the public key uses the two keys to encrypt and decrypt the data

- Public-key cryptography allows the users to hide the data that they want to send. The sender encrypts the data and the receiver decrypts the data. The encrypted message is not understood by unauthorized users.

Concept of keys: Public key and Private key

The cryptographic keys are the most essential element in public-key cryptography. Without the function and significance of keys, there is not much left to understand in public-key cryptography. So, let us learn the concept of keys!

As we know, we use a pair of keys i.e. *Public key* and *Private key* in public-key cryptography. Both of these keys are generated using the Elliptic Curve cryptography method. Firstly, it creates the private key and then it creates a public key from the private key using the *Elliptic Curve Algorithm (*aka *ECDSA)*. Therefore, both the private and public keys are cryptographically and mathematically linked to each other.

There is an important thing to note here, i.e. the process of generating a public key from the private key is irreversible. That is, we can obtain the corresponding public key from its private key but we cannot obtain the private key from its public key. The algorithm is designed in such a way that it requires a lot of computational power and time to brute force the private key which is next to impossible.

This algorithm helps in keeping the private key private and untraceable from the public key. Because a node in the blockchain network can only carry out transactions within the network. It is possible if its private key is kept secret and its public key which others know in the network.

The private and public keys are of a certain length depending on the algorithm used to create them. Usually, the key length is 256 bits or can fall in the range of 1024 to 2048 bits. Now, the length of the public key seems a little too long for us to easily distribute it in the network. So, we need to create a shorter public address from the public key using a hashing function. Here, the public key is like an email address and public address is like the username. It is obvious that sharing your username with others is easier than sharing the entire email address.

Just like how we cannot compute a private key from its public key, we cannot compute a public key from the public address. Public address (also called a Bitcoin address in a Bitcoin network) is the first thing that we need if two nodes want to carry out a transaction on the blockchain network.

Therefore, in Public-key cryptography the most important elements are a private key, a public key, and the public address. All of this information is kept secure in a software known as *Wallet*. A digital wallet is independent of the blockchain network. It stores the important information of a blockchain node such as its address, private key, the public key, and transaction balance.

Let us learn about the private and public key in a little more detail.

1. Private Key

A private key is a long series of alphanumeric characters that is unique for every individual user or node in the blockchain network. A private key is like a password which if shared can give away our confidential information. So, we must keep our private key confidential from the network.

The digital wallets (software or hardware) essentially store the private key as its security is very important. The usual format for storing the key is a wallet import format which has a 51 character long key. This length may vary depending upon the storage formats.

The **two main functions of a private key** in providing security in a blockchain network are:

a. The private key is used to decrypt a message that the sender encrypts using the public key (of the receiver). This ensures that the intended receiver gets the encrypted message and is safe from other users on the way. Once the message reaches the receiver intact, he decrypts it into a readable format using his private key.

b. Another important function of the private key is securing the message or information by digital signature. A digital signature is used to verify a blockchain transaction. In the digital signature, the message is signed using the sender’s private key. In this way, the receiver can verify that the message (using the sender’s public key) is actually sent by the sender and not someone else.

2. Public Key

A public key is the counterpart of a private key as it is cryptographically derived from it. A public key is available for all the nodes in the network. This helps in the verification of a transaction by all the nodes in a blockchain network. Let’s suppose that you are a node in the network and you want to send a message or information to another node.

To carry out a secure transaction you will sign the message from your private key and send it for verification from the entire network. Each node can access your public key and so they will verify the transaction as authentic and pass it. When all the nodes verify your transaction using your public key the transaction can take place. Generally, a public address is used for transactions rather than the public key because of its length. The public key is long and not easily shareable. So, a shorter version of it is created by hashing which is the public address.

The **two main functions of a public key** in providing security in a blockchain network are:

a. To encrypt a message or information using the public key of the receiver. This ensures that only the receiver who has its corresponding private key can decrypt and read the message.

b. To verify if the sender is authentic by confirming the digital signature. A digital signature is done by the sender's private key. A public key verifies the sender's identity by matching (complementing) with his private key.

Digital signatures in blockchain

After the private key and public key, another important aspect of public-key cryptography is the digital signature. No transaction in a blockchain network is secure if it is not digitally signed by the sender's private key. The cryptography i.e. the encryption done using the public and private keys ensures that the information we are sending to other nodes is safe and no one in the middle can read or change it.

Whereas, the purpose of doing a digital signature before sending the information is to state authority over the information and tokens (cryptocurrency). It is like signing a cheque where you state that it is your money that you are giving from your authorized bank account.

Similarly, when you digitally sign the information you send in a blockchain network, you say that you are an authorized node. And you rightfully own the tokens or currency you wish to give to someone in the network. Therefore, the digital signature proves the ownership of the funds and the account and protects them from forgery.

Now, let us learn how digital signatures are done.

Before we start understanding the entire process of digital signatures, we must know which algorithm is used to create digital signatures. Similar to the private and public key, digital signature is created by the *Elliptic Curve Digital Signature Algorithm* (*ECDSA*). An important thing to note here is that ECDSA is not based on encryption. This means that the keys are not encrypted, only the message or information that we are sending is encrypted.

This algorithm applies itself in two parts;

1. In the first part, it takes the private key and Merkel root (hash) of the transaction and creates the signature by mathematical computations. Then this signed transaction is sent out to other users on the blockchain network. They will all verify the signature of the sending node using the second part of the algorithm.

2. In the second part, other nodes compute a binary result using the digital signature of the sender, the transaction information, and the public key of the sender. If the mathematical algorithm gives the result as True, then it is verified that the sender has sent the message from an authentic node.

All the validating nodes or computers in the network will verify the digital signature by using the sender's public key.

How does Public-key cryptography work?

Now that we are through with all the important concepts related to public-key cryptography. Let us move on to understand the entire process of public-key cryptography. And how does it work to secure and verify a transaction on the blockchain.

Suppose you are a legitimate node on a blockchain network. Now, you need to have three things in order to carry out secure transactions within the network; a private key, a public key, and a wallet address, or a public address. For this, you need to install a blockchain wallet software that will automatically create a pair of private key and public key and a wallet address. This software is an independent platform from the blockchain. It gives you a digital identity and a safe place to keep your keys.

Furthermore, your public address (aka wallet address) is like a mailbox and your private key is like the key of that mailbox. Your mailbox or its address is known to everyone and anyone can send you things using the mailbox. But, only you can open your mailbox and access the contents inside it using the key to the mailbox. Similarly, anyone within the blockchain network can send you tokens or messages to your public address. But only you can decrypt and read that message using your private key.

Let us summarize the working of public-key cryptography with the help of a situation. Here Raj wants to send a message to Aditi on a blockchain network. We call this exchange of information between two nodes on the blockchain a "*transaction*".

Step 1: Raj will take the message that he wants to share and encrypt it using Aditi's public key or public address. This will convert the message into an unreadable format.

Step 2: Raj will now take the hashed message and sign this message using his private key. This is known as digitally signing the transaction (digital signature).

Step 3: Now, Raj is ready to send this message to Aditi via the blockchain network. But before this, Raj needs to get this transaction verified by the entire blockchain network. Using Raj's public key, every node on the network will verify the digital signature of Raj and pass the transaction.

Step 4: After successful verification, Aditi will receive the message but in an encrypted form known as ciphertext. First off, Aditi will also verify the digital signature of Raj using his public key or public address.

Step 5: Then, Aditi will decrypt the ciphertext using her private key. This will convert the message into a readable format.

Step 6: The transaction is successfully carried out. Also, it is recorded on a new block in the blockchain permanently. No one can deny that this transaction between Raj and Aditi did not take place.

Benefits of Public Key Cryptography

Public key cryptography promises a lot of security benefits in an open network like blockchain. Three most important aspects, as well as benefits of using public-key cryptography as the security method, are; *Confidentiality*, *Integrity*, and *Authenticity*.

1. Confidentiality: Blockchain assures confidentiality of the data that we are sharing by using a pair of keys. The public and private keys that are linked to each other make sure that the data or information that we are sending is kept secret from others. It maintains confidentiality by encrypting the data using a public key and decrypting it on the other end using its corresponding private key.

2. Integrity: Public-key cryptography also maintains the integrity of the data by encrypting the data. Due to end encryption, no one except for the sender and the receiver has access to the information. So, one can be sure that the data is intact and no one has changed it in the middle.

3. Authenticity: Another important aspect and a major benefit of public-key encryption is the authenticity of the user. Because it uses digital signatures in every transaction, it is impossible for some to fake their identity. That is why every node on the blockchain network can be sure that the sender is an authentic part of the network. This is how blockchain builds trust amongst its users.

Limitations of Public Key Cryptography

Just like everything has a downside to it, there are a few limitations of public-key cryptography.

1. The ability of mathematical algorithms to encrypt and decrypt data or messages is limited to only a certain size of data. If there are large amounts of data that need to be encrypted the algorithm runs slow. This slows down the process of encryption and demands greater computational power.

2. If someone has access to the secret private key or accidentally exposes it to the network. All the data encrypted using that private key will be in the wrong hands. One cannot restore or re-encrypt the data once the private key is out.

3. If a node loses its private key, its data will forever be stuck and they cannot make transactions from the same public address again. Such a node will not be able to access the data encrypted by its private key.

Difference between Public and Private blockchain

S.no	Basis of Comparison	Public BlockChain	Private BlockChain
1.	Access	In this type of blockchain anyone can read, write and participate in a blockchain. Hence, it is permissionless blockchain. It is public to everyone.	In this type of blockchain read and write is done upon invitation, hence it is a permissioned blockchain.
2.	Network Actors	Don’t know each other	Know each other
3.	Decentralized Vs Centralized	A public blockchain is decentralized.	A private blockchain is more centralized.
4.	Order Of Magnitude	The order of magnitude of a public blockchain is lesser than that of a private blockchain as it is lighter and provides transactional throughput.	The order of magnitude is more as compared to the public blockchain.
5.	Native Token	Yes	Not necessary
6.	Speed	Slow	Fast

7.	Transactions pre second	Transactions per second are lesser in a public blockchain.	Transaction per second is more as compared to public blockchain.
8.	Security	A public network is more secure due to decentralization and active participation. Due to the higher number of nodes in the network, it is nearly impossible for ‘bad actors’ to attack the system and gain control over the consensus network.	A private blockchain is more prone to hacks, risks, and data breaches/ manipulation. It is easy for bad actors to endanger the entire network. Hence, it is less secure.
9.	Energy Consumption	A public blockchain consumes more energy than a private blockchain as it requires a significant amount of electrical resources to function and achieve network consensus.	Private blockchains consume a lot less energy and power.
10.	Consensus algorithms	Some are proof of work, proof of stake, proof of burn, proof of space etc.	Proof of Elapsed Time (PoET), Raft, and Istanbul BFT can be used only in case of private blockchains.
11.	Attacks	In a public blockchain, no one knows who each validator is and this increases the risk of potential collision or a 51% attack (a group of miners which control more than 50% of the network’s computing power.).	In a private blockchain, there is no chance of minor collision. Each validator is known and they have the suitable credentials to be a part of the network.
12.	Effects	Potential to disrupt current business models through disintermediation. There is lower infrastructure cost. No need to maintain servers or system admins radically. Hence reducing the cost of creating and running decentralized application (dApps).	Reduces transaction cost and data redundancies and replace legacy systems, simplifying documents handling and getting rid of semi manual compliance mechanisms.
13.	Examples	Bitcoin, Ethereum, Monero, Zcash, Dash, Litecoin, Stellar, Steemit etc.	R3 (Banks), EWF (Energy), B3i (Insurance), Corda.